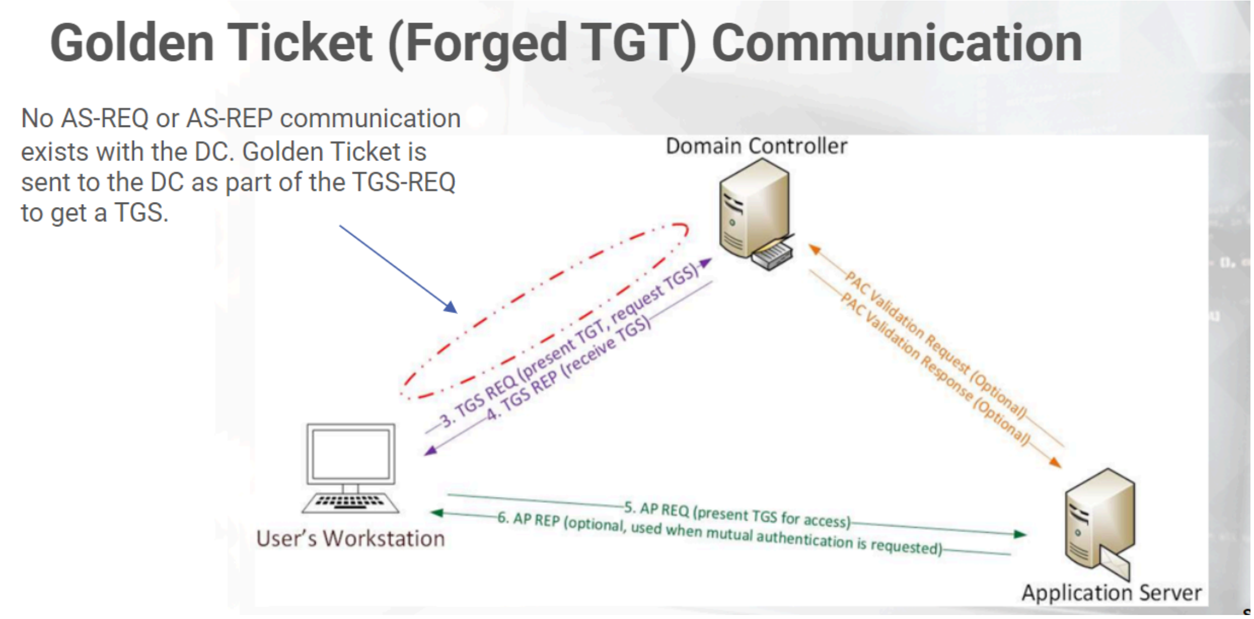
Golden Tickets:

Golden ticket is forget TGT Kerberos ticket that can be used to request TGS ticket for any service on any computer. Mean this ticket allow the attacker to have access to any thing they want within the network.

Golden ticket creation requirements:

- Domain Name
- Domain SID
- Domain KRBTGT Account NTLM password hash
- User ID for impersonation even non-existing users

Mean here the attacker can use the KRBTGT account hash that is responsible for Granting tickets for users, will use that account to grant them self any kind of ticket they want. And to get this KRBTGT account hash, the attacker need to compromise the Domain control like have admin access to it and then read the NTDS.dit file which have all the hash for all the users and then it can grab that hash and use it to grant them self any kind of Ticket they want.


Golden Ticket (Forged TGT) Communication

No AS-REQ or AS-REP communication exists with the DC. Golden Ticket is sent to the DC as part of the TGS-REQ to get a TGS.

Domain Controller
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

This means that attacker will not need to authenticate as a user, they will just give them self a golden ticket with a user ID they want to impersonate or non-existing user, and then they can use that ticket to request the TGS ticket so they can access services. As this ticket is privileged that allow the attacker to have access to anything, so they will get a TGS that gain them full access to that Service or resource that its TGS was requested.

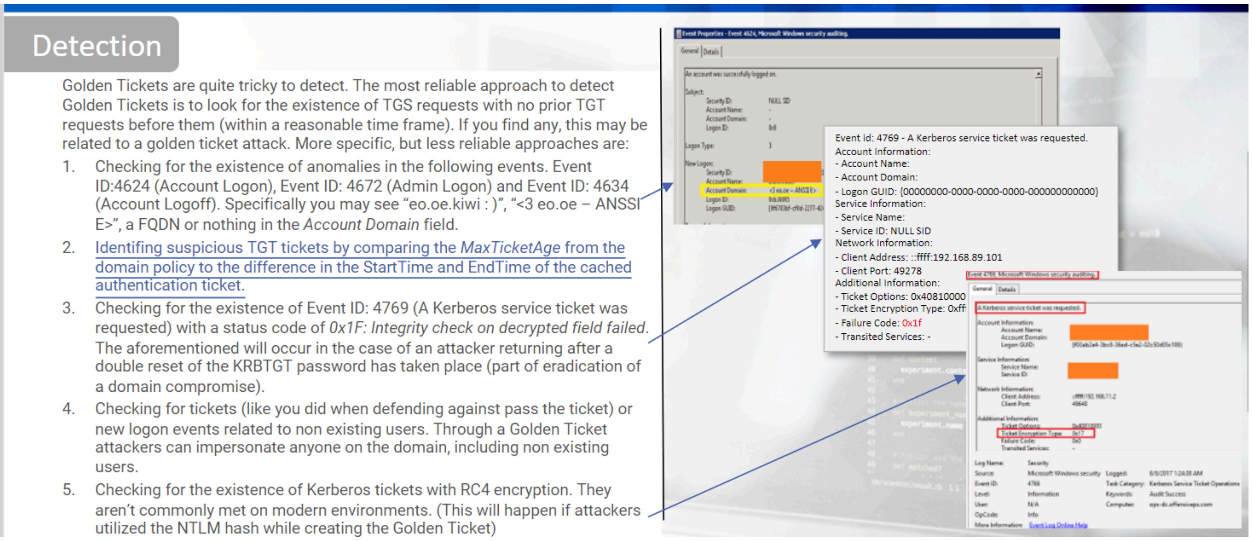
Golden ticket is powerful, it allows the attacker to compromise anything in the network by getting the full access, like compromise any domain in the forest, and they can do this by abusing the SID history attribute, SID history gives ability to include in a Golden ticket or Silver one in any group in the AD forest and use it for authorization. So that mean attacker can abuse the SID attribute to include the Golden ticket or the Silver ticket in any AD forest domains group like the admins group, and then use that ticket for authorization in the entire forest.

The attacker uses the SID History attribute to make the ticket appear as if the user is a member of a specific group, such as the admin group.

For example an attacker gain access to the KRBTGT account password has, it can leverage its SID history, and then add the entire forest enterprise admins group to the Golden ticket, mean making the ticket valid in all domains leading to compromise of the Parent Domain.

Detection:

As at first we said that the attacker will not need to authenticate as any user, they just give them self a ticket with any user ID to impersonate them. So we can hunt for any TGS request where there is not TGT request prior to it, mean we will look for any ticket that was obtained without the TGT request, like the user didn't authenticated to get the TGT and then Request the TGS, as that's how the Golden ticket is obtained. If we find any TGT that was obtained without the TGT request then it can be suspicious.



Detection

Golden Tickets are quite tricky to detect. The most reliable approach to detect Golden Tickets is to look for the existence of TGS requests with no prior TGT requests before them (within a reasonable time frame). If you find any, this may be related to a golden ticket attack. More specific, but less reliable approaches are:

1. Checking for the existence of anomalies in the following events. Event ID:4624 (Account Logon), Event ID: 4672 (Admin Logon) and Event ID: 4634 (Account Logoff). Specifically you may see "eo.oe.kiwi :)", "<3 eo.oe – ANSSI E>", a FQDN or nothing in the *Account Domain* field.
2. Identifing suspicious TGT tickets by comparing the *MaxTicketAge* from the domain policy to the difference in the StartTime and EndTime of the cached authentication ticket.
3. Checking for the existence of Event ID: 4769 (A Kerberos service ticket was requested) with a status code of *0x1F: Integrity check on decrypted field failed.* The aforementioned will occur in the case of an attacker returning after a double reset of the KRBTGT password has taken place (part of eradication of a domain compromise).
4. Checking for tickets (like you did when defending against pass the ticket) or new logon events related to non existing users. Through a Golden Ticket attackers can impersonate anyone on the domain, including non existing users.
5. Checking for the existence of Kerberos tickets with RC4 encryption. They aren't commonly met on modern environments. (This will happen if attackers utilized the NTLM hash while creating the Golden Ticket)

Event Properties - Event 4624, Microsoft Windows security auditing.

General | Details

```
An account was successfully logged on.

Subject:
        Security ID:        NULL SID
        Account Name:       -
        Account Domain:     -
        Logon ID:           0x0

Logon Type:                 3

New Logon:
        Security ID:        [redacted]
        Account Name:
        Account Domain:     <3 eo.oe – ANSSI E>
        Logon ID:           0xb36005
        Logon GUID:         {8f6703bf-cf8d-2277-42
```

```
Event id: 4769 - A Kerberos service ticket was requested.
Account Information:
- Account Name:
- Account Domain:
- Logon GUID: {00000000-0000-0000-0000-000000000000}
Service Information:
- Service Name:
- Service ID: NULL SID
Network Information:
- Client Address: ::ffff:192.168.89.101
- Client Port: 49278
Additional Information:
- Ticket Options: 0x40810000
- Ticket Encryption Type: 0xff
- Failure Code: 0x1f
- Transited Services: -
```

Event 4769, Microsoft Windows security auditing.

General | Details

```
A Kerberos service ticket was requested.

Account Information:
        Account Name:       [redacted]
        Account Domain:
        Logon GUID:         {f03ab2a4-3bc8-36ad-c5a2-02c50d05c189}

Service Information:
        Service Name:       [redacted]
        Service ID:

Network Information:
        Client Address:     ::ffff:192.168.11.2
        Client Port:        49648

Additional Information:
        Ticket Options:     0x40810000
        Ticket Encryption Type:  0x17
        Failure Code:       0x0
        Transited Services: -

Log Name:      Security
Source:        Microsoft Windows security   Logged:         8/6/2017 1:24:38 AM
Event ID:      4769                         Task Category:  Kerberos Service Ticket Operations
Level:         Information                  Keywords:       Audit Success
User:          N/A                          Computer:       ops-dc.offensiveps.com
OpCode:        Info
More Information:  Event Log Online Help
```

1: Read the one Above, its important.

3: One thing to note, when we are recovering form the domain compromise, we have to reset the KRBTG account 2 times, the reason is to make the tickets that are given invalid. And if the attackers comes back to the network and try to use the golden ticket to get the TGS service ticket, we can check the Event ID 4769 (Kerberos service Ticket was requested) with status code of "0x1f" (decrypted field failed), this means the attacker used a invalid ticket to get a service TGS ticket to gain access to service but it failed as the ticket wasn't decrypted as the KRBTGT hash was changed.

4: like we said in the golden ticket, there is the user ID filed which indicates for which user this ticket is built for and attacker can impersonate any user and they might put a user ID that dosnt exist so if we see a non existing user logon attempts , it can indicate the golden ticket.

5: if the attacker used the NTLM hash while creating the golden ticket, then the encryption used for the creating is RC4 which in modern environment we don't use the RC4

Read the screen shot above